AWS Cloud Infrastructure VAPT Report (Sample for ISO 27001 Compliance)

Client: MyFinTech Cloud Pvt Ltd
Date: 06-Sep-2025
Prepared by: SecureOps VAPT Team
Scope: AWS Production (VPC, EC2, RDS, S3, IAM, EKS, Lambda, ALB, CloudFront)
Compliance Reference: ISO 27001, OWASP Top 10, NIST 800-53, CIS AWS Benchmarks

---

1. Executive Summary

- **Total Assets Tested:** 40+
- **Total Vulnerabilities Found:** 52
- Critical: 5
- High: 15
- Medium: 18
- Low: 14
- **Overall Risk:** HIGH
- **Business Impact:** Potential data leakage, privilege escalation, insecure configurations.

---

2. Detailed Findings

🔴Critical (5)

#	Asset	Vulnerability	CVE	Impact	Recommendation
1	S3 prod-customer-data	Publicly accessible	N/A	Data leak	Apply bucket policies, encryption
2	IAM User devops-admin	Full admin key exposed	N/A	Full AWS compromise	Rotate keys, use roles + MFA
3	EC2 bastion	SSH exposed to 0.0.0.0/0	N/A	Brute-force attack	Restrict CIDR
4	RDS customer-db	Unencrypted at rest	N/A	Data breach	Enable AES-256 encryption
5	Lambda order-processing	Privilege escalation via environment variables	N/A	AWS takeover	Limit IAM role, encrypt env vars

🔶High (15)

#	Asset	Vulnerability	CVE	Impact	Recommendation
6	Security Group web	Open port 80/443 to all	N/A	Network exposure	Restrict CIDRs
7	EC2 app-prod	Outdated AMI	CVE-2021-41190	Remote exploit	Patch AMI
8	EKS cluster	Node runs as root	N/A	Container compromise	Use non-root user
9	CloudFront	TLS 1.0 enabled	N/A	Weak encryption	Enable TLS 1.2+
10	IAM Role dev	Overprivileged	N/A	Privilege escalation	Reduce permissions
11	EC2 web-prod	Default SSH key in AMI	N/A	Unauthorized access	Remove default keys
12	RDS analytics	Public endpoint enabled	N/A	Data access	Disable public endpoint
13	S3 logs-bucket	No versioning	N/A	Data recovery risk	Enable versioning
14	Lambda image-processor	Old runtime	N/A	Vulnerable to exploits	Update runtime
15	EC2 redis-cache	Unpatched Redis	CVE-2022-0543	RCE	Update Redis version
16	S3 backup	Weak ACL	N/A	Data exposure	Restrict ACLs
17	ALB web	HTTP redirect misconfigured	N/A	MITM risk	Force HTTPS
18	EC2 bastion	Weak password policy	N/A	Brute-force	Enforce strong password
19	IAM user ci-cd	No MFA	N/A	Account takeover	Enable MFA
20	EKS worker	Unrestricted access to API	N/A	Cluster compromise	Apply RBAC restrictions

🟡Medium (18)

#	Asset	Vulnerability	CVE	Impact	Recommendation
21	S3 prod-media	No encryption in transit	N/A	Data exposure	Enable HTTPS
22	Lambda billing	No timeout	N/A	DOS risk	Set timeout
23	RDS replica	Backups unencrypted	N/A	Data exposure	Enable encrypted backups
24	EC2 log-server	Weak SSH cipher	N/A	MITM	Use strong cipher
25	CloudTrail	Not integrated with CloudWatch	N/A	Audit gap	Enable integration
26	S3 audit-logs	Public read access	N/A	Data exposure	Restrict access
27	IAM group devs	Excess privileges	N/A	Privilege escalation	Limit permissions
28	Lambda notifications	Environment variables plaintext	N/A	Data leak	Encrypt variables
29	EKS kube-system	Default service accounts	N/A	Privilege escalation	Remove default accounts
30	EC2 monitoring	Outdated agent	N/A	Metrics loss	Update agent
31	S3 temp-files	No lifecycle policy	N/A	Storage bloat	Configure lifecycle
32	ALB app	Security headers missing	N/A	XSS risk	Add headers
33	RDS dev	Weak password	N/A	Unauthorized access	Enforce strong password
34	Lambda worker	IAM policy wildcard	N/A	Privilege escalation	Restrict IAM
35	EC2 backup	Unpatched kernel	CVE-2023-12345	RCE	Patch kernel
36	S3 logs	Unencrypted	N/A	Data exposure	Enable SSE
37	EKS node	Docker outdated	CVE-2022-3150	Container compromise	Update Docker
38	CloudFront	CORS misconfigured	N/A	Data leak	Correct CORS

🟢Low (14)

#	Asset	Vulnerability	CVE	Impact	Recommendation
39	EC2 dev	Weak SSH banner	N/A	Recon	Update banner
40	S3 temp	Missing tagging	N/A	Cost tracking	Tag resources
41	IAM user test	No password rotation	N/A	Policy non-compliance	Rotate passwords
42	Lambda temp	Logging disabled	N/A	Audit gap	Enable logging
43	EC2 old-app	HTTP only	N/A	MITM	Enable HTTPS
44	RDS test	Old engine minor version	N/A	Vulnerabilities	Update engine
45	EKS temp	Unrestricted pod access	N/A	Privilege escalation	Restrict RBAC
46	S3 logs	ACL misconfigured	N/A	Info disclosure	Fix ACLs
47	EC2 cache	No monitoring	N/A	Audit gap	Enable monitoring
48	CloudFront	Weak caching	N/A	Performance	Adjust caching policy
49	Lambda analytics	Unrestricted triggers	N/A	DOS risk	Restrict triggers
50	RDS old-dev	Old snapshot	N/A	Data leak	Delete old snapshots
51	IAM temp	Too many policies	N/A	Policy sprawl	Consolidate policies
52	EC2 staging	Weak sysctl	N/A	Kernel attack	Harden sysctl

3. Recommendations

- Immediate remediation for **Critical + High vulnerabilities**.
- Medium/Low issues can be scheduled in routine patch cycles.
- Enforce **CIS AWS benchmark** across all accounts.
- Automate **Terrascan + Trivy + OWASP Dependency-Check + Cost Estimation** in CI/CD.
- Continuous compliance monitoring for **ISO 27001**.

Prepared by SecureOps VAPT Team
For Internal Use Only